



RECEIVED

FEB 19 2003

APPENDIX B:

Technology Center 2100

CLEAN VERSION OF ALL PENDING CLAIMS AS NOW PRESENTED

Sub 17. (Three Times Amended) A method for establishing cryptographic communications, comprising the steps of:

encoding a plaintext message word  $M$  to a ciphertext word  $C$ , wherein  $M$  corresponds to a number representative of a message and wherein

$$0 \leq M \leq n-1,$$

wherein  $n$  is a composite number formed by the product of  $p_1 \cdot p_2 \cdot \dots \cdot p_k$ ,  $k$  is an integer greater than 2 and  $p_1, p_2, \dots, p_k$  are distinct random prime numbers,  $C$  is a number representative of an encoded form of message word  $M$ , and wherein said encoding step comprises transforming said message word  $M$  to said ciphertext word  $C$ , whereby

$$C \equiv M^e \pmod{n},$$

and wherein  $e$  is a number relatively prime to  $(p_1-1), (p_2-1), \dots$ , and  $(p_k-1)$ ; and

decoding said ciphertext word  $C$  to a receive message word  $M'$ , said decoding step being performed using a decryption exponent  $d$  that is defined by

$$d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$$

said decoding step including the further steps of,

defining a plurality of  $k$  sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$\vdots$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$\vdots$

$$C_k \equiv C \pmod{p_k},$$

27  $d_1 \equiv d \pmod{(p_1 - 1)},$   
 28  $d_2 \equiv d \pmod{(p_2 - 1)},$  and  
 29  $\vdots$   
 30  $d_k \equiv d \pmod{(p_k - 1)},$   
 31 solving said sub-tasks to determine results  $M_1', M_2', \dots, M_k',$  and  
 32 combining said results of said sub-tasks to produce said receive message word  $M',$   
 33 wherein  $M' = M.$

1 18. A method as recited in claim 17 wherein said step of combining said results of said sub-  
 2 tasks includes a step of performing a recursive combining process to produce said receive  
 3 message word  $M'.$

1 19. A method as recited in claim 18 wherein said recursive combining process is performed  
 2 in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n,$$

wherein  $2 \leq i \leq k,$  and

$$M' = Y_k, Y_1 = M_1', \text{ and } w_i = \prod_{j=1}^i p_j.$$

1 20. A method as recited in claim 17 wherein said step of combining said results of said sub-  
 2 tasks includes a step of performing a summation process to produce said receive message word  
 3  $M'.$

1 21. A method as recited in claim 20 wherein said summation process is performed in  
 2 accordance with

$$M' \equiv \sum_{i=1}^k M_i' (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j=1}^i p_j.$$

22. (Three Times Amended) A cryptographic communications system for establishing communications, comprising:

a communication medium;

encoding means coupled to said communication medium and adapted for transforming a transmit message word M to a ciphertext word C and for transmitting said ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$ , wherein n is a composite number of the form,

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

wherein k is an integer greater than 2 and  $p_1, p_2, \dots, p_k$  are distinct random prime numbers, and wherein said ciphertext word C corresponds to a number representative of an enciphered form of said message word M and corresponds to

$$C \equiv M^e \pmod{n},$$

wherein e is a number relatively prime to  $(p_1-1), (p_2-1), \dots$ , and  $(p_k-1)$ ; and

decoding means communicatively coupled with said communication medium for receiving said ciphertext word C via said medium, said decoding means being operative to perform a decryption process for transforming said ciphertext word C to a receive message word M', wherein M' corresponds to a number representative of a deciphered form of C, said decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \pmod{((p_1-1)(p_2-1)\dots(p_k-1))},$$

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$\vdots$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$\vdots$

$$\begin{aligned}
30 \quad & C_k \equiv C \pmod{p_k}, \\
31 \quad & \\
32 \quad & d_1 \equiv d \pmod{(p_1 - 1)}, \\
33 \quad & d_2 \equiv d \pmod{(p_2 - 1)}, \\
34 \quad & \vdots \\
35 \quad & d_k \equiv d \pmod{(p_k - 1)},
\end{aligned}$$

36 solving said sub-tasks to determine results  $M_1', M_2', \dots, M_k'$ , and

37 combining said results of said sub-tasks to produce said receive message word  $M'$

38 whereby  $M' = M$ .

23. A cryptographic communications system as recited in claim 22 wherein said decoding means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said receive message word  $M'$ .

24. A cryptographic communications system as recited in claim 23 wherein said decoding means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n,$$

wherein  $2 \leq i \leq k$ , and

$$M' = Y_k, Y_1 = M_1', \text{ and } w_i = \prod_{j < i} p_j.$$

25. A cryptographic communications system as recited in claim 22 wherein said decoding means is operative combine said results of said sub-tasks by performing a summation process to produce said receive message word  $M'$ .

26. A cryptographic communications system as recited in claim 25 wherein said decoding means is operative to perform said summation process accordance with

$$M' \equiv \sum_{i=1}^k M_i' (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j=1}^i p_j.$$

27. (Three Times Amended) A method for establishing cryptographic communications, comprising the step of:

encoding a plaintext message word  $M$  to a ciphertext word  $C$ , wherein  $M$  corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

$n$  being a composite number formed from the product of  $p_1 \cdot p_2 \cdot \dots \cdot p_k$ , wherein  $k$  is an integer greater than 2 and  $p_1, p_2, \dots, p_k$  are distinct random prime numbers, and wherein the ciphertext word  $C$  is a number representative of an encoded form of message word  $M$ , wherein said step of encoding includes the steps of

defining a plurality of  $k$  sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

25 wherein  $e$  is a number relatively prime to  $(p_1-1)$ ,  $(p_2-1)$ , ..., and  $(p_k-1)$ ,  
26 solving said sub-tasks to determine results  $C_1, C_2, \dots, C_k$ , and  
27 combining said results of said sub-tasks to produce said ciphertext word  $C$ .

1 28. A method as recited in claim 27 wherein said step of combining said results of said sub-  
2 tasks includes a step of performing a recursive combining process to produce said ciphertext  
3 word  $C$ .

1 29. A method as recited in claim 28 wherein said recursive combining process is performed  
2 in accordance with

3 
$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n,$$

4 wherein  $2 \leq i \leq k$ , and

5 
$$C = Y_k, Y_1 = C_1, \text{ and } w_i = \prod_{j=1}^i p_j.$$

1 30. A method as recited in claim 27 wherein said step of combining said results of said sub-  
2 tasks includes a step of performing a summation process to produce said ciphertext word  $C$ .

1 31. A method as recited in claim 30 wherein said summation process is performed in  
2 accordance with

3 
$$C \equiv \sum_{i=1}^k C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

4 where

5 
$$w_i = \prod_{j=1}^i p_j.$$

1 32. (Three Times Amended) A cryptographic communications system for establishing  
2 communications, comprising:  
3 a communication medium;

4 encoding means coupled to said communication medium and operative to transform a  
5 transmit message word M to a ciphertext word C, and to transmit said ciphertext word C on said  
6 medium, wherein M corresponds to a number representative of a message, and

7  $0 \leq M \leq n-1,$

8 n being a composite number formed from the product of  $p_1 \cdot p_2 \cdot \dots \cdot p_k$  wherein k is an integer  
9 greater than 2 and  $p_1, p_2, \dots, p_k$  are distinct random prime numbers, and wherein the ciphertext  
10 word C is a number representative of an encoded form of message word M, said encoding means  
11 being operative to transform said transmit message word M to said ciphertext word C by  
12 performing an encoding process comprising the steps of

13 defining a plurality of k sub-tasks in accordance with

14  $C_1 \equiv M_1^{e_1} \pmod{p_1},$

15  $C_2 \equiv M_2^{e_2} \pmod{p_2},$

16  $\vdots$

17  $C_k \equiv M_k^{e_k} \pmod{p_k},$

18 where

19  $M_1 \equiv M \pmod{p_1},$

20  $M_2 \equiv M \pmod{p_2},$

21  $\vdots$

22  $M_k \equiv M \pmod{p_k},$

23  $e_1 \equiv e \pmod{(p_1 - 1)},$

24  $e_2 \equiv e \pmod{(p_2 - 1)},$  and

25  $\vdots$

26  $e_k \equiv e \pmod{(p_k - 1)},$

27 wherein e is a number relatively prime to  $(p_1-1), (p_2-1), \dots,$  and  $(p_k-1),$   
28 solving said sub-tasks to determine results  $C_1, C_2, \dots, C_k,$  and  
29 combining said results of said sub-tasks to produce said ciphertext word C.  
30

1 33. A cryptographic communications system as recited in claim 32 wherein said encoding  
2 means is operative to combine said results of said sub-tasks by performing a recursive combining  
3 process to produce said ciphertext word C.

1 34. A cryptographic communications system as recited in claim 33 wherein said encoding  
2 means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n,$$

4 wherein  $2 \leq i \leq k$ , and

$$C = Y_k, Y_1 = C_1, \text{ and } w_i = \prod_{j=i} p_j.$$

1 35. A cryptographic communications system as recited in claim 32 wherein said encoding  
2 means is operative to combine said results of said sub-tasks by performing a summation process  
3 to produce said message word C.

1 36. A cryptographic communications system as recited in claim 35 wherein said encoding  
2 means is operative to perform said summation process in accordance with

$$C \equiv \sum_{i=1}^k C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

4 where

$$w_i = \prod_{j=i} p_j.$$

1 37. (Three Times Amended) A method for establishing cryptographic communications,  
2 comprising the steps of:

3 decoding a ciphertext word C to a message word M, wherein M corresponds to a number  
4 representative of a message and wherein

$$0 \leq M \leq n-1$$

6 wherein n is a composite number formed by the product of  $p_1 p_2 \dots p_k$ , k is an integer greater  
7 than 2 and  $p_1, p_2, \dots, p_k$  are distinct random prime numbers, C is a number representative of an



8 encoded form of message word M that is encoded by transforming said message word M to said  
9 ciphertext word C whereby

10  $C \equiv M^e \pmod{n},$

11 and wherein e is a number relatively prime to  $(p_1-1)$ ,  $(p_2-1)$ , ..., and  $(p_k-1)$ ;

12 said decoding step being performed using a decryption exponent d that is defined by

13  $d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$

14 wherein said step of decoding includes the steps of

15 defining a plurality of k sub-tasks in accordance with

16  $M_1 \equiv C_1^{d_1} \pmod{p_1},$

17  $M_2 \equiv C_2^{d_2} \pmod{p_2},$

18  $\vdots$

19  $M_k \equiv C_k^{d_k} \pmod{p_k},$

20 wherein

21  $C_1 \equiv C \pmod{p_1},$

22  $C_2 \equiv C \pmod{p_2},$

23  $\vdots$

24  $C_k \equiv C \pmod{p_k},$

25  $d_1 \equiv d \pmod{(p_1 - 1)},$

26  $d_2 \equiv d \pmod{(p_2 - 1)},$  and

27  $\vdots$

28  $d_k \equiv d \pmod{(p_k - 1)},$

29 solving said sub-tasks to determine results  $M_1, M_2, \dots, M_k$ , and

30 combining said results of said sub-tasks to produce said message word M.

31  
1 38. A method as recited in claim 37 wherein said step of combining said results of said sub-  
2 tasks includes a step of performing a recursive combining process to produce said message word  
3 M.

1 39. A method as recited in claim 38 wherein said recursive combining process is performed  
2 in accordance with

3 
$$Y_i \equiv Y_{i-1} + [(M_i - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n,$$

4 wherein  $2 \leq i \leq k$ , and

5 
$$M' = Y_k, Y_i = M'_i, \text{ and } w_i = \prod_{j < i} p_j.$$

1 40. A method as recited in claim 37 wherein said step of combining said results of said sub-  
2 tasks includes a step of performing a summation process to produce said message word M.

1 41. A method as recited in claim 40 wherein said summation process is performed in  
2 accordance with

3 
$$M \equiv \sum_{i=1}^k M_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

4 where

5 
$$w_i = \prod_{j \neq i} p_j.$$

1 42. (Three Times Amended) A cryptographic communications system for establishing  
2 communications, comprising:  
3 a communication medium;  
4 decoding means communicatively coupled with said communication medium for  
5 receiving a ciphertext word C via said medium, and being operative to transform said ciphertext  
6 word C to a receive message word M', wherein a message M corresponds to a number  
7 representative of a message and wherein,

8 
$$0 \leq M \leq n-1$$

9 wherein n is a composite number formed by the product of  $p_1 \cdot p_2 \cdot \dots \cdot p_k$ , k is an integer greater  
10 than 2 and  $p_1, p_2, \dots, p_k$  are distinct random prime numbers, and wherein said ciphertext word C  
11 is a number representative of an encoded form of said message word M that is encoded by  
12 transforming M to said ciphertext word C whereby,

13  $C \equiv M^e \pmod{n}$ ,  
14 and wherein  $e$  is a number relatively prime to  $(p_1-1)$ ,  $(p_2-1)$ , ..., and  $(p_k-1)$ ;  
15 said decoding means being operative to perform a decryption process using a decryption  
16 exponent  $d$  that is defined by

$$d \equiv e^{-1} \pmod{(p_1-1)(p_2-1) \dots (p_k-1)},$$

18 said decryption process including the steps of

19 defining a plurality of  $k$  sub-tasks in accordance with,

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

22  $\vdots$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

24 wherein,

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

27  $\vdots$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

32  $\vdots$

$$d_k \equiv d \pmod{(p_k - 1)},$$

34 solving said sub-tasks to determine results  $M_1'$ ,  $M_2'$ , ...,  $M_k'$ , and  
35 combining said results of said sub-tasks to produce said receive message word  $M'$ ,  
36 whereby  $M'=M$ .

1 43. A cryptographic communications system as recited in claim 42 wherein said decoding  
2 means is operative to combine said results of said sub-tasks by performing a recursive combining  
3 process to produce said receive message word  $M'$ .

44. A cryptographic communications system as recited in claim 41 wherein said decoding means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n,$$

wherein  $2 \leq i \leq k$ , and

$$M = Y_k, Y_1 = M_1', \text{ and } w_i = \prod_{j < i} p_j.$$

45. A cryptographic communications system as recited in claim 42 wherein said decoding means is operative to combine said results of said sub-tasks by performing a summation process to produce said receive message word  $M'$ .

46. A cryptographic communications system as recited in claim 45 wherein said decoding means is operative to perform said summation process in accordance with

$$M' \equiv \sum_{i=1}^k M_i' (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

47. (Three Times Amended) A method for generating a digital signature, comprising the step of:

signing a plaintext message word  $M$  to create a signed ciphertext word  $C$ , wherein  $M$  corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

$n$  being a composite number formed from the product of  $p_1 \cdot p_2 \cdot \dots \cdot p_k$ , wherein  $k$  is an integer greater than 2 and  $p_1, p_2, \dots, p_k$  are distinct random prime numbers, and wherein the signed ciphertext word  $C$  is a number representative of a signed form of message word  $M$ , wherein

$$C \equiv M^d \pmod{n}, \text{ and}$$

wherein said step of signing includes the steps of defining a plurality of  $k$  sub-tasks in accordance with

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

13  $C_2 \equiv M_2^{d_2} \pmod{p_2},$

14  $\vdots$

15  $C_k \equiv M_k^{d_k} \pmod{p_k},$

16 where

17  $M_1 \equiv M \pmod{p_1},$

18  $M_2 \equiv M \pmod{p_2},$

19  $\vdots$

20  $M_k \equiv M \pmod{p_k},$

21

22  $d_1 \equiv d \pmod{(p_1 - 1)},$

23  $d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$

24  $\vdots$

25  $d_k \equiv d \pmod{(p_k - 1)},$

26 wherein  $d$  is defined by

27  $d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}, \text{ and}$

28  $e$  is a number relatively prime to  $(p_1 - 1), (p_2 - 1), \dots, \text{ and } (p_k - 1),$

29 solving said sub-tasks to determine results  $C_1, C_2, \dots, C_k,$  and

30 combining said results of said sub-tasks to produce said ciphertext word  $C$ .

1 48. A method as recited in claim 47 wherein said step of combining said results of said sub-  
2 tasks includes a step of performing a recursive combining process to produce said ciphertext  
3 word  $C$ .

1 49. A method as recited in claim 48 wherein said recursive combining process is performed  
2 in accordance with

3  $Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1}) (w_i^{-1} \pmod{p_i}) \pmod{p_i}] \cdot w_i \pmod{n},$

4 wherein  $2 \leq i \leq k,$  and

5

$$C = Y_k, Y_1 = C_1, \text{ and } w_i = \prod_{j=1}^i p_j.$$

1 50. A method as recited in claim 47 wherein said step of combining said results of said sub-  
 2 tasks includes a step of performing a summation process to produce said signed ciphertext word  
 3 C.

1 51. A method as recited in claim 50 wherein said summation process is performed in  
 2 accordance with

$$C \equiv \sum_{i=1}^k C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

4 where

$$w_i = \prod_{j=1}^i p_j.$$

1 52. (Three Times Amended) A digital signature generation system, comprising:  
 2 a communication medium;  
 3 digital signature generating means coupled to said communication medium and operative  
 4 to transform a transmit message word M to a signed ciphertext word C, and to transmit said  
 5 signed ciphertext word C on said medium, wherein M corresponds to a number representative of  
 6 a message, and

$$0 \leq M \leq n-1,$$

8 n being a composite number formed from the product of  $p_1 \cdot p_2 \cdot \dots \cdot p_k$  wherein k is an integer  
 9 greater than 2 and  $p_1, p_2, \dots, p_k$ , are distinct random prime numbers, and wherein the signed  
 10 ciphertext word C is a number representative of a signed form of said message word M, wherein

$$C \equiv M^d \pmod{n},$$

12 said digital signature generating means being operative to transform said transmit  
 13 message word M to said signed ciphertext word C by performing a digital signature generating  
 14 process comprising the steps of,

15 defining a plurality of k sub-tasks in accordance with,

16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$

$\vdots$

$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where,

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$\vdots$

$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$\vdots$

$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by,

$$d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}, \text{ and}$$

e is a number relatively prime to  $(p_1 - 1)$ ,  $(p_2 - 1)$ , ..., and  $(p_k - 1)$ ,

solving said sub-tasks to determine results  $C_1, C_2, \dots, C_k$ , and

combining said results of said sub-tasks to produce said signed ciphertext word C.

53. A digital signature generation system as recited in claim 52 wherein said signature generating means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said signed ciphertext word C.

54. A digital signature generation system as recited in claim 53 wherein said digital signature generating means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1}) (w_i^{-1} \pmod{p_i}) \pmod{p_i}] \cdot w_i \pmod{n},$$

wherein  $2 \leq i \leq k$ , and

$$C = Y_k, Y_i = C_i, \text{ and } w_i = \prod_{j=i} p_j.$$

55. A digital signature generation system as recited in claim 52 wherein said signature generating means is operative to combine said results of said sub-tasks by performing a summation process to produce said signed message word C.

56. A digital signature system as recited in claim 55 wherein said signature generating means is operative to perform said summation process in accordance with

$$C \equiv \sum_{i=1}^k C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j=i} p_j.$$

57. (Three Times Amended) A digital signature process, comprising the steps of:  
signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of  $p_1 \cdot p_2 \cdot \dots \cdot p_k$ , k is an integer greater than 2 and  $p_1, p_2, \dots, p_k$  are distinct random prime numbers, C is a number representative of a signed form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C whereby,

$$C \equiv M^d \pmod{n},$$

wherein d is defined by

$$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)), \text{ and}$$

e is a number relatively prime to  $(p_1 - 1), (p_2 - 1), \dots$ , and  $(p_k - 1)$ ; and

verifying said ciphertext word C to a receive message word M' by performing the steps

of,



15 defining a plurality of k sub-tasks in accordance with

16  $M_1' \equiv C_1^{e_1} \pmod{p_1},$

17  $M_2' \equiv C_2^{e_2} \pmod{p_2},$

18  $\vdots$

19  $M_k' \equiv C_k^{e_k} \pmod{p_k},$

20 wherein

21  $C_1 \equiv C \pmod{p_1},$

22  $C_2 \equiv C \pmod{p_2},$

23  $\vdots$

24  $C_k \equiv C \pmod{p_k},$

25  $e_1 \equiv e \pmod{(p_1 - 1)},$

26  $e_2 \equiv e \pmod{(p_2 - 1)},$  and

27  $\vdots$

28  $e_k \equiv e \pmod{(p_k - 1)},$

30 solving said sub-tasks to determine results  $M_1', M_2', \dots, M_k'$ , and

31 combining said results of said sub-tasks to produce said receive message word  $M'$ ,

32 whereby  $M' = M$ .

1 58. A digital signature process as recited in claim 57 wherein said step of combining said  
2 results of said sub-tasks includes a step of performing a recursive combining process to produce  
3 said receive message word  $M'$ .

1 59. A digital signature process as recited in claim 58 wherein said recursive combining  
2 process is performed in accordance with

3  $Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1}) (w_i^{-1} \pmod{p_i}) \pmod{p_i}] \cdot w_i \pmod{n},$

4 wherein  $2 \leq i \leq k$ , and

5

$$M' = Y_k, Y_i = M'_i, \text{ and } w_i = \prod_{j \neq i} p_j.$$

1 60. A digital signature process as recited in claim 58 wherein said step of combining said  
2 results of said sub-tasks includes a step of performing a summation process to produce said  
3 receive message word  $M'$ .

1 61. A digital signature process as recited in claim 60 wherein said summation process is  
2 performed in accordance with

$$M' \equiv \sum_{i=1}^k M'_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

4 where

$$w_i = \prod_{j \neq i} p_j.$$

1 62. (Three Times Amended) A digital signature system, comprising:

2 a communication medium;

3 digital signature generating means coupled to said communication medium and adapted

4 for transforming a message word  $M$  to a signed ciphertext word  $C$  and for transmitting said

5 signed ciphertext word  $C$  on said medium, wherein  $M$  corresponds to a number representative of a  
6 message, and

7  $0 \leq M \leq n-1$ , wherein  $n$  is a composite number of the form

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k,$$

9 wherein  $k$  is an integer greater than 2 and  $p_1, p_2, \dots, p_k$  are distinct random prime

10 numbers, and wherein said signed ciphertext word  $C$  corresponds to a number representative of a

11 signed form of said message word  $M$  and corresponds to

$$C \equiv M^d \pmod{n},$$

13 wherein  $d$  is defined by

$$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)), \text{ and}$$

15  $e$  is a number relatively prime to  $(p_1 - 1), (p_2 - 1), \dots$ , and  $(p_k - 1)$ ; and

16 digital signature verification means communicatively coupled with said communication  
17 medium for receiving said signed ciphertext word C via said medium, and being operative to  
18 verify said signed ciphertext word C by performing the steps of,  
19 defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

22  $\vdots$

$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

24 wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

27  $\vdots$

$$C_k \equiv C \pmod{p_k},$$

$$e_1 \equiv e \pmod{p_1 - 1},$$

$$e_2 \equiv e \pmod{p_2 - 1},$$

32  $\vdots$

$$e_k \equiv e \pmod{p_k - 1},$$

34 solving said sub-tasks to determine results  $M_1', M_2', \dots M_k'$ , and  
35 combining said results of said sub-tasks to produce said receive message word  $M'$   
36 wherein  $M'=M$ .

1 63. A digital signature system as recited in claim 62 wherein said decoding means is  
2 operative to combine said results of said sub-tasks by performing a recursive combining process  
3 to produce said receive message word  $M'$ .

1 64. A digital signature system as recited in claim 63 wherein said decoding means is  
2 operative to perform said recursive combining process in accordance with

3  $Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n,$

4 wherein  $2 \leq i \leq k$ , and

5  $M' = Y_k$ ,  $Y_1 = M_1'$ , and  $w_i = \prod_{j < i} p_j$ .

1 65. A digital signature system as recited in claim 62 wherein said decoding means is  
2 operative combine said results of said sub-tasks by performing a summation process to produce  
3 said receive message word  $M'$ .

1 66. A digital signature system as recited in claim 65 wherein said decoding means is  
2 operative to perform said summation process accordance with

F/ 3  $M' \equiv \sum_{i=1}^k M_i' (w_i^{-1} \bmod p_i) w_i \bmod n,$

4 where

5  $w_i = \prod_{j \neq i} p_j.$

Sub G2 73. A method as recited in claim 17 wherein said step of solving said sub-tasks includes  
2 processing each of said sub-tasks by an associated one of a plurality of exponentiator units  
3 operating substantially simultaneously.

1 74. A method as recited in claim 17 wherein each of said distinct random prime number has  
2 the same number of bits.

1 75. A cryptographic communications system as recited in claim 22 wherein said step of  
2 solving said sub-tasks includes processing each of said sub-tasks by an associated one of a  
3 plurality of exponentiator units operating substantially simultaneously.

1 76. A cryptographic communications system as recited in claim 22 wherein each of said  
2 distinct random prime number has the same number of bits.

1 77. A method as recited in claim 27 wherein said step of solving said sub-tasks includes  
2 processing each of said sub-tasks by an associated one of a plurality of exponentiator units  
3 operating substantially simultaneously.

1 78. A method as recited in claim 27 wherein each of said distinct random prime number has  
2 the same number of bits.

1 79. A cryptographic communications system as recited in claim 32 wherein said step of  
2 solving said sub-tasks includes processing each of said sub-tasks by an associated one of a  
3 plurality of exponentiator units operating substantially simultaneously.

F 1 80. A cryptographic communications system as recited in claim 32 wherein each of said  
2 distinct random prime number has the same number of bits.

1 81. A method as recited in claim 37 wherein said step of solving said sub-tasks includes  
2 processing each of said sub-tasks by an associated one of a plurality of exponentiator units  
3 operating substantially simultaneously.

1 82. A method as recited in claim 37 wherein each of said distinct random prime number has  
2 the same number of bits.

1 83. A cryptographic communications system as recited in claim 42 wherein said step of  
2 solving said sub-tasks includes processing each of said sub-tasks by an associated one of a  
3 plurality of exponentiator units operating substantially simultaneously.

1 84. A cryptographic communications system as recited in claim 42 wherein each of said  
2 distinct random prime number has the same number of bits.

1 85. A method as recited in claim 47 wherein said step of solving said sub-tasks includes  
2 processing each of said sub-tasks by an associated one of a plurality of exponentiator units  
3 operating substantially simultaneously.

1 86. A method as recited in claim 47 wherein each of said distinct random prime number has  
2 the same number of bits.

1 87. A digital signature generation system as recited in claim 52 wherein said step of solving  
2 said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of  
3 exponentiator units operating substantially simultaneously.

F 1 88. A digital signature generation system as recited in claim 52 wherein each of said distinct  
2 random prime number has the same number of bits.

1 89. A digital signature process as recited in claim 57 wherein said step of solving said sub-  
2 tasks includes processing each of said sub-tasks by an associated one of a plurality of  
3 exponentiator units operating substantially simultaneously.

1 90. A digital signature process as recited in claim 57 wherein each of said distinct random  
2 prime number has the same number of bits.

1 91. A digital signature system as recited in claim 62 wherein said step of solving said sub-  
2 tasks includes processing each of said sub-tasks by an associated one of a plurality of  
3 exponentiator units operating substantially simultaneously.

1 92. A digital signature system as recited in claim 62 wherein each of said distinct random  
2 prime number has the same number of bits.